UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/814,426	03/21/2001	Timothy S. DeBruine	1104-041	4082

74548 7590 09/24/2008
FlashPoint Technology and Withrow & Terranova
100 Regency Forest Drive
Suite 160
Cary, NC 27518

EXAMINER	
DIVECHA, KAMAL B	

ART UNIT	PAPER NUMBER
2151	

MAIL DATE	DELIVERY MODE
09/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/814,426
Filing Date: March 21, 2001
Appellant(s): DEBRUINE ET AL.

Anthony J. Josephson
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/28/08 appealing from the Office action mailed 4/4/08 (Final Rejection).

(1) Real Party in Interest

The statement containing the Real Party in Interest is contained in the Brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Teodosiu et al., US 2002/0062336 A1

Araujo, US 6,393,488 B1

Dutta et al., US 6,636,854 B2

Lopke, US 6,553,310 B1

Yau et al., US 2002/0066026 A1

Oguchi et al., US 6,304,912 B1

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

<u>ART REJECTION I:</u>

Claims 1-7, 9, 13-19, 21, 25-31, 33 and 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teodosiu et al. (hereinafter Teodosiu, US 2002/0062336 A1) in view of Araujo (US 6,393,488 B1).

As per claim 1, Teodosiu discloses a method for optimizing private network file transfers in a peer-to-peer public network, the peer-to-peer public network including a server and a plurality of nodes, wherein at least two of the plurality of nodes are part of the same private network (fig. 1 and pg. 9 [0124]: Peer to Peer network **over LAN environment**), the method comprising the steps of:

(a) receiving by the server a search request from a first node of the plurality of nodes in the peer-to-peer public network for a file (fig. 2 item #210, fig. 4 item #410, pg. 4 [0045]: receiving a resource request);

(b) determining by the server that the file is stored on a second node of the plurality of nodes in the peer-to-peer network (fig. 2 item #240, fig. 4 item #430, pg. 4 [0047-0049]: searching for locations that stores requested resource. Teodosiu also determines closest second node); and

(d) sending instructions by the server to the first node to request the file from the second node, such that the second node transfers the file to the first node over the private network (fig. 4 item #460, 425, pg. 3 [0035-0037], pg. 4 [0045-0053], pg. 6 [0077-0081]).

However, Teodosiu does not disclose the process of (c) determining by the server that the first and second nodes are part of the same private network.

Araujo discloses the process of determining by the server if the first device is included in the same LAN, i.e. same private network, as the second device (fig. 5 item #511, col. 7 L13-65: determining whether the two nodes are within the same LAN and/or determining whether first and second node are part of the same LAN).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Teodosiu in view of Araujo in order to determine whether the first and second node, which are part of the peer to peer network, are part of the same private network.

One of ordinary skilled in the art would have been motivated because it would have resolved the client's request locally (Araujo: col. 7 L13-41: by returning the IP address of the local node; Teadosiu: [0047]: **optimize traffic**).

As per claim 2, Teodosiu in view of Araujo discloses the process of registering a client IP address, a subnet mask, and a peer IP address of both the first and second node with the server

(Araujo: col. 5 L41-67, fig. 4, col. 6 L34 to col. 7 L13: a mapping table including client local IP address and global IP address, i.e. Peer IP address; a subnet mask is usually associated with an IP address, see fig 5 item #514, 515).

As per claim 3, Teodosiu in view of Araujo discloses the process of registering with the server whether the network address translation has been performed on the first and second nodes and whether the first and second nodes are directly reachable from other nodes on the public network or unreachable (Araujo: col. 5 L41-67, col. 6 L34 to col. 7 L65: a mapping table indicates whether the translation is performed or not and/or whether the nodes are reachable or not).

As per claim 4, Teodosiu in view of Araujo discloses the process of determining that NAT has been performed on a particular node when the nodes client IP address does not match the nodes peer IP address (Araujo: col. 6 L34 to col. 7 L65: If the client IP address is different than global IP address, then logically, the two different addresses for a client device suggests the usage of NAT).

As per claim 5, Teodosiu in view of Araujo discloses the process of determining that a particular node is directly reachable from other nodes on the public network when the server can connect with the node using the node's client IP address (Araujo: col. 6 L34 to col. 7 L65, col. 8 L24 to col. 9 L45: nodes are directly reachable if the NAT determines no translation is required).

As per claim 6, Teodosiu in view of Araujo discloses the process of storing the client IP address, a subnet mask, and a peer IP address of both the first and second nodes in a node registry (Araujo: col. 5 L41-67, fig. 4, col. 6 L34 to col. 7 L13: a mapping table including client

local IP address and global IP address, i.e. Peer IP address; a subnet mask is usually associated with an IP address).

As per claim 7, Teodosiu discloses the process further including the process of allowing a user of the first node to enter search terms for finding a particular file (pg. 4 [0045]: a peer device enters the resource request, i.e. search request, [0053]).

As per claim 9, Teodosiu in view of Araujo discloses the process of determining that the second node is part of the same private network as the first node, and therefore locally reachable by the first node, when the NAT has not been performed on either the first and second nodes and the subnet Ids of each first and second nodes match (Araujo: fig. 5 item #514, col. 7 L13-65).

As per claims 13-19, 21, 25-31, 33 and 37-40, they do not teach or further define over the limitations in claims 1-7 and 9. Therefore claims 13-19, 21, 25-31, 33 and 37-40 are rejected for the same reasons as set forth in claims 1-7 and 9.

Claims 8, 10, 12, 20, 22, 24, 32, 34, 36, 41 and 43-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teodosiu et al. (hereinafter Teodosiu, US 2002/0062336 A1) in view of Araujo (US 6,393,488 B1), and further in view of Dutta et al. (hereinafter Dutta, US 6,636,854 B2).

As per claim 8, Teodosiu and Araujo does not disclose the process further including the process of querying a database containing file names with the search terms to find the file names matching the search terms, and identifying nodes containing the matching file, including the second node.

Dutta explicitly discloses the process including the process of querying a database containing file names with the search terms to find the file names matching the search terms, and identifying nodes containing the matching file, including the second node (fig. 5A, fig. 5c, fig. 6A step #608, col. 7 L15 to col. 8 L15, col. 8 L59 to col. 9 L56).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Teodosiu and Araujo in view of Dutta in order to querying a database containing file names with the search terms to find the file names matching the search terms, and identifying nodes containing the matching file, including the second node.

One of ordinary skilled in the art would have been motivated because it would have enabled the server to search and present the results associated with the search item (Dutta: col. 9 L9-67).

As per claim 10, Teodosiu and Araujo does not disclose the process of returning a list of search results from the server to the first node, where the list includes the identities and addresses of the matching nodes, IP addresses and subnet masks.

Dutta discloses the process of returning a list of search results from the server to the first node including the addresses of the matching nodes (fig. 5A, fig. 5c, fig. 6A step #608, col. 7 L15 to col. 8 L44, col. 8 L59 to col. 9 L56: URLS are associated with IP addresses and IP addresses are associated with subnet masks, col. 10 L35-45).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Teodosiu and Araujo in view of Dutta in order to return a list of search results from the server to the first node, where the list includes the identities and addresses of the matching nodes, IP addresses and subnet masks.

One of ordinary skilled in the art would have been motivated so that the user can retrieve the document or the file associated with the search hit (Dutta: col. 9 L32-67).

As per claim 12, Teodosiu in view of Araujo does not discloses the process of sending the client IP address of the second node to the first node such that the first node sends request for the file to the second node using the client IP address of the second node and sending the file from the second node to the first node using the client IP address of the first node.

Dutta discloses the process of sending the client IP address of the second node to the first node such that the first node sends request for the file to the second node using the client IP address of the second node and sending the file from the second node to the first node using the client IP address of the first node (col. 5 L10-63, col. 6 L13 to col. 7 L29).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Teodosiu and Araujo in view of Dutta in order to sending the client IP address of the second node to the first node such that the first node sends request for the file to the second node using the client IP address of the second node and sending the file from the second node to the first node using the client IP address of the first node.

One of ordinary skilled in the art would have been motivated so that the client can retrieve the file from the other node (Dutta: col. 6 L57-67).

As per claims 22, 24, 32, 34, 36, 41 and 43-47, they do not teach or further define over the limitations in claims 8, 10 and 12. Therefore, claims 22, 24, 32, 34, 36, 41 and 43-47 are rejected for the same reasons as set forth in claims 8, 10 and 12.

Claims 11, 23, 35 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teodosiu et al. (hereinafter Teodosiu, US 2002/0062336 A1) in view of Araujo (US 6,393,488 B1), further in view of Dutta et al. (hereinafter Dutta, US 6,636,854 B2), and further in view of Lopke (hereinafter Lopke, US 6,553,310 B1).

As per claim 11, Teodosiu, Araujo in view of Dutta does not disclose the process of sorting the search results by locally reachable nodes followed by the directly reachable nodes.

Lopke discloses the process of sorting the information servers based on its location and/or proximity (col. 3 L25-46).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Teodosiu, Araujo and Dutta in view of Lopke in order to sort the results by locally reachable nodes followed by the directly reachable nodes.

One of ordinary skilled in the art would have been motivated because it would have notified the requestor of the closest node capable of satisfying the request.

As per claims 23, 35 and 42, they do not teach or further define over the limitations in claim 11. Therefore, claims 23, 35 and 42 are rejected for the same reasons as set forth in claim 11.

ART REJECTION II:

Claims 1, 7, 8, 13, 19, 20, 25, 31 and 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1).

As per claim 1, Dutta discloses a peer-to-peer public network including a server and a plurality of nodes, wherein at least two of the plurality of nodes are part of the same private network (applicant admitted prior art, specification, pg. 3 lines 8-15), the method comprising the steps of:

(a) receiving by the server a search request from a first node of the plurality of nodes in the peer-to-peer public network for a file (col. 5 L10-63, col. 6 L13 to col. 7 L29: Gnutella peer to peer network);

(b) determining by the server that the file is stored on a second node of the plurality of nodes in the peer-to-peer network (col. 5 L10-63, col. 6 L13 to col. 7 L29: determining a node having the file); and

(d) sending instructions by the server to the first node to request the file from the second node, such that the second node transfers the file to the first node (col. 5 L10-63, col. 6 L13 to col. 7 L29: sending the address for the node having the file).

However, Dutta does not disclose the process of (c) determining by the server that the first and second nodes are part of the same private network.

Yau discloses the process of optimizing private network file transfers and the process of determining by the server that the first and second nodes are part of the same private network by determining that the source node having the file and client node requesting the file are located

behind the same firewall and the process of sending instructions by the server to the first node to request the file from the second node, such that the second node transfers the file to the first node over the private network (pg. 2 [0018-0019], fig. 2: private network protected by firewall, pg. 5 [0067], [0070-0074]: determining that two nodes are located within the same firewall and/or private internal network, and pg. 3 [0042]).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Dutta in view of Yau in order to determine whether the first and second node are part of the same private network.

One of ordinary skilled in the art would have been motivated because it allows the system to take advantage of the higher speeds usually achieved by subnets and to aid in the ability to propagate data throughout subnets (Yau: pg. 5 [0072], [0067], pg. 2 [0018-0019]).

As per claim 7, Dutta discloses the process of allowing a user of the first node to enter search terms for finding a particular file (col. 5 L10-63, col. 6 L13-65).

As per claim 8, Dutta discloses the process of querying a database containing file names with the search terms to find file names matching the search terms, and identifying nodes containing the matching file, including the second node (col. 5 L10-63, col. 6 L13-65).

As per claims 13, 19, 20, 25, 31 and 44-46, they do not teach or further define over the limitations in claims 1, 7 and 8. Therefore claims 13, 19, 20, 25, 31 and 44-46 are rejected for the same reasons as set forth in claims 1, 7 and 8.

Claims 2, 6, 14, 26, 30 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1), and further in view of Oguchi et al. (hereinafter Oguchi, US 6,304,912 B1).

As per claim 2, Dutta in view of Yau discloses the process of registering a client IP address and a Peer IP address of both the first and second nodes with the server (Dutta: col. 8 L15-54: note peer ip address may simply be client ip address).

However, Dutta in view of Yau does not disclose registering, i.e. storing, a subnet mask of both the first and second nodes.

Oguchi teaches the process of storing subnet mask of the nodes (fig. 3B item #s21, fig. 13-15, col. 8 L47-67).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Dutta and Yau in view of Oguchi in order to register the subnet mask of the nodes.

One of ordinary skilled in the art would have been motivated because subnet mask indicates which portion of the network-layer address of the one of the at least one second communication apparatus indicates the one of the plurality of subnetworks to which the one of the at least one second communication apparatus belongs (Oguchi: col. 8 L47-67).

As per claims 6, 14, 26, 30 and 32, they do not teach or further define over the limitations in claim 2. Therefore claims 6, 14, 26, 30 and 32 are rejected for the same reasons as set forth in claim 2.

Claims 3-5, 9-10, 12, 15-18, 21-22, 24, 27- 29 and 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1), further in view of Oguchi et al. (hereinafter Oguchi, US 6,304,912 B1), and further in view of Araujo (US 6,393,488 B1).

As per claim 3, Dutta, Yau and Oguchi does not disclose the process of registering with the server whether the network address translation has been performed on the first and second nodes and whether the first and second nodes are directly reachable from other nodes on the public network or unreachable.

Araujo discloses the process of registering with the server whether the network address translation has been performed on the first and second nodes and whether the first and second nodes are directly reachable from other nodes on the public network or unreachable (Araujo: col. 5 L41-67, col. 6 L34 to col. 7 L65: a mapping table indicates whether the translation is performed or not and/or whether the nodes are reachable or not based on the local and global IP addresses).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Dutta, Yau and Oguchi in view of Araujo in order to register with the server of the reachability information of the nodes.

One of ordinary skilled in the art would have been motivated because it would have indicated whether the nodes are reachable through local or global IP address and/or it would have enabled the communication between the LAN and the Internet (Araujo: col. 6 L46 to col. 7 L13, col. 1 L21-30).

As per claim 4, Dutta, Yau, Oguchi in view of Araujo discloses the process of determining that NAT has been performed on a particular node when the nodes client IP address does not match the nodes peer IP address (Araujo: col. 6 L34 to col. 7 L65: If the client IP address is different than global IP address, then logically, it implies the presence and usage of the NAT service).

As per claim 5, Dutta, Yau, Oguchi in view of Araujo discloses the process of determining that a particular node is directly reachable from other nodes on the public network when the server can connect with the node using the node's client IP address (Yau: pg. 5 [0069-0075], pg. 3 [0042]: uses the client IP address to communicate with public network logically implies that the nodes are directly reachable from public network; Araujo: col. 6 L34 to col. 7 L65, col. 8 L24 to col. 9 L45: nodes are directly reachable if the NAT determines no translation is required).

As per claim 9, Dutta, Yau, Oguchi in view of Araujo discloses the process of determining that the second node is part of the same private network as the first node, and therefore locally reachable by the first node, when the NAT has not been performed on either the first and second nodes and the subnet Ids of each first and second nodes match (Araujo: fig. 5 item #514, col. 7 L13-65; Yau: pg. 5 [0069-0074]: NAT is not performed, and matching the subnet id by comparing the IP address of nodes).

As per claim 10, Dutta discloses the process of returning a list of search results from the server to the first node including the addresses of the matching nodes (fig. 5A, fig. 5c, fig. 6A step #608, col. 7 L15 to col. 8 L44, col. 8 L59 to col. 9 L56: URLS are associated with IP addresses and IP addresses are associated with subnet masks, col. 10 L35-45).

As per claim 12, Dutta discloses the process of sending the client IP address of the second node to the first node such that the first node sends request for the file to the second node using the client IP address of the second node and sending the file from the second node to the first node using the client IP address of the first node (Dutta: col. 5 L10-63, col. 6 L13 to col. 7 L29; Yau: pg. 5 [0069-0074] and pg. 3 [0042]).

As per claims 15-18, 21-22, 24, 27- 29 and 33-36, they do not teach or further define over the limitations in claims 3-5, 9 and 12. Therefore claims 15-18, 21-22, 24, 27- 29 and 33-36 are rejected for the same reasons as set forth in claims 3-5, 9 and 12.

Claims 11, 23 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1), further in view of Oguchi et al. (hereinafter Oguchi, US 6,304,912 B1), further in view of Araujo (US 6,393,488 B1), and further in view of Lopke (US 6,553,310 B1).

As per claim 11, Dutta, Yau, Oguchi and Araujo does not disclose the process of sorting the search results by locally reachable nodes followed by the directly reachable nodes.

Lopke discloses the process of sorting the information servers based on its location and/or proximity (col. 3 L25-46).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Dutta, Yau, Oguchi, Araujo in view of Lopke in order to sort the results by locally reachable nodes followed by the directly reachable nodes.

One of ordinary skilled in the art would have been motivated because it would have notified the requestor of the closest node capable of satisfying the request.

As per claims 23 and 35, they do not teach or further define over the limitations in claim 11. Therefore, claims 23 and 35 are rejected for the same reasons as set forth in claim 11.

Claims 37 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1), and further in view of Araujo (US 6,393,488 B1).

As per claim 37, it does not teach or further define over the limitations in claims 1, 3 and 9. Therefore claim 37 is rejected for the same reasons as in claims 1, 3 and 9.

As per claim 47, Dutta explicitly discloses the process of receiving by the server the search request from the first node including at leas tone search item identifying the file and the process of querying a database relating each one of a number of files including the file and at least one of the plurality of nodes in the peer to peer public nework storing the one of the number of files using the at least one search term to identify at least one of the plurality of ndoes including the second node storing the file (fig. 5A, fig. 5c, fig. 6A step #608, col. 7 L15 to col. 8 L15, col. 8 L59 to col. 9 L56).

Claims 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1), further in view of Araujo (US 6,393,488 B1), and further in view of Oguchi et al. (hereinafter Oguchi, US 6,304,912 B1).

As per claims 38-41, they do not teach or further define over the limitations in claims 2, 4, 5 and 10, respectively. Therefore claims 38-41 are rejected for the same reasons as set forth in claims 2, 4, 5 and 10, respectively.

Claims 42 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al. (hereinafter Dutta, US 6,636,854 B2) in view of Yau et al. (hereinafter Yau, US 2002/0066026 A1), further in view of Araujo (US 6,393,488 B1), further in view of Oguchi et al. (hereinafter Oguchi, US 6,304,912 B1), and further in view of Lopke (US 6,553,310 B1).

As per claims 42 and 43, they do not teach or further define over the limitations in claims 11 and 12, respectively. Therefore claims 42 and 43 are rejected for the same reasons as set forth in claims 11 and 12, respectively.

(10) Response to Argument

Examiner summarizes various arguments raised by the appellant, and addresses each of them individually.

In the Brief, appellant argues in substance that:

a. None of the references, either alone or in combination, disclose or suggest determining by a server that first and second nodes, which are part of a peer-to-peer network, are also part of a same private network (Brief, pg. 11 paragraph D. 1, 12-13).

In response to argument [a], Examiner respectfully disagrees.

<u>Independent claim 1 recites:</u>

> A method for optimizing private network file transfers in a peer-to-peer public network, the peer-to-peer public network including a server and a plurality of nodes, wherein at least two of the plurality of nodes are part of a same private network, the method comprising the steps of:
> (a) receiving by the server a search request from a first node of the plurality of nodes in the peer-to-peer public network for a file;
> (b) determining by the server that the file is stored on a second node of the plurality of nodes in the peer-to-peer network;
> (c) determining by the server that the first and second nodes are part of the same private network; and
> (d) sending instructions by the server to the first node to request the file from the second node, such that the second node transfers the file to the first node over the same private network.

Initially, **Appellant's Background of Invention Discloses (pg. 3 lines 8-15):**

> Although peer networks are effective, current peer networks-have inefficiencies. **For example, it is not uncommon for a peer-to-peer network to have peers that are part of a private network, such as a local area network (LAN), for instance.** When a peer requests a file from another peer, the file transfer typically occurs over the Internet, even when the two peers are within the same private network. In a peer-to-peer network that includes many private networks and many file transfers occurring within the same private network, transferring the file over the Internet is costly and wastes limited bandwidth.

In other words, it's well know that peer to peer network have peers or users that are part of a same private network, i.e. same private network. That is, two or more users from same LAN can participate in peer to peer network.

Teodosiu et al.

Teodosiu discloses a peer to peer public network such as shown by REALM 150 comprising plurality of peers such as peers 140 connected to servers through a network environment, e.g. see fig. 1 reproduced herein.

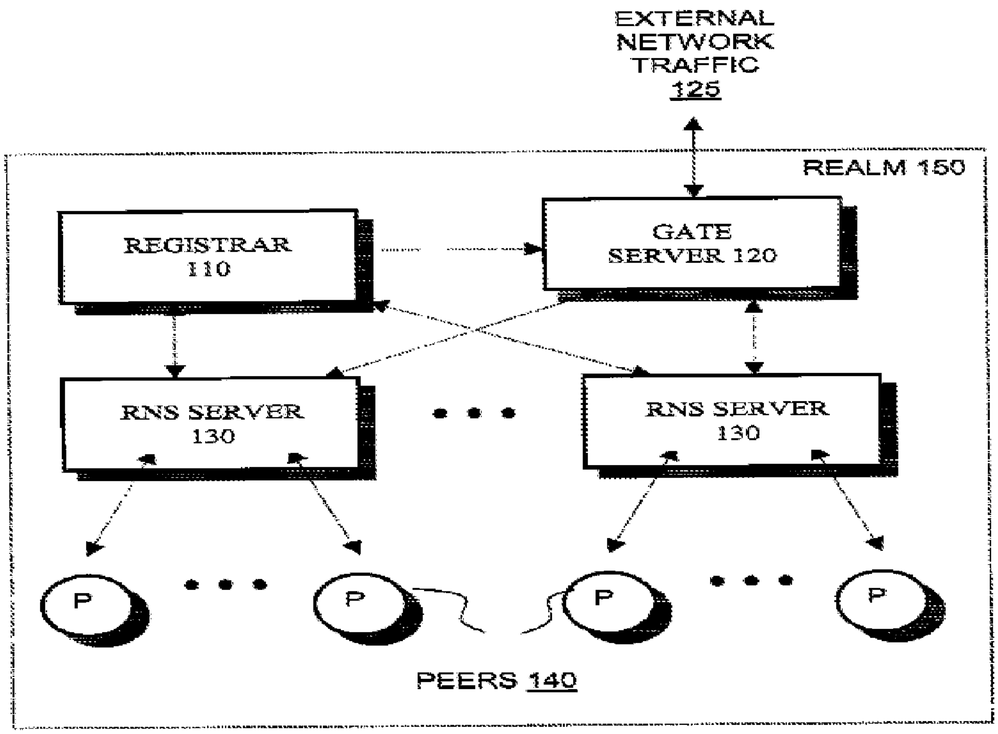

FIG. 1

Teodosiu further discloses:

[0124] In FIG. 1, the elements in realm 150 communicate with one another using any of a variety of network transmission protocols, such as the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP), and any of a variety of application protocols, such as a proprietary protocol, the Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), or the like. The networking environment including realm 150 may comprise a local area network (LAN), a wide area network (WAN), a private

internet, the public Internet, or the like. In alternate embodiments, realm 150 may comprise a standalone network.

In other words, the network environment on which the peer to peer network, i.e. realm 150, is implemented **includes a LAN, i.e. a private network.**

Clearly, peers 140 as in fig. 1, which are part of the peer to peer network such as realm 150, are also part of the same private network such as LAN.

Furthermore, Teodosiu, in one embodiment, discloses:

Locating Resources

[0044] **FIG. 2** illustrates one embodiment of locating a resource in more detail. The illustrated embodiment is from the perspective of an RNS server, although a gate server may perform similar functions. **FIG. 2** includes a number of implementation specific details. Other embodiments may not include all of the elements illustrated in **FIG. 2**, may perform elements in a different order, and may include additional elements.

[0045] First, the RNS server **130** receives, from a peer **140** or from the gate server **120**, a resource request at **210** for the location of a particular resource. The request uniquely identifies a resource and a master publisher of the resource within the realm to which this RNS server belongs. The request can take any number of forms from a messaging protocol specific to this particular locator service to a universally accepted protocol such as HTTP.

[0046] At **220**, the RNS server checks its own memory to determine if it has a resource record corresponding to the requested resource. In one embodiment, resource records comprise unique identifiers for resources and master publishers as well as one or more locations where the resources are expected to be located. The record may also indicate whether or not particular locations are expected to be active (logged into the network or not). In which case, the RNS server compares the unique identifier from the request to the list of recorded unique identifiers.

[0047] If the RNS server does have a matching record, the RNS server assumes that the record is current. If the record lists an active location for the resource, the RNS server responds in **230** with the resource status and a set of locations. The record may list zero or more active locations where the resource has been cached. If the record lists more than one active location for the resource, the RNS server may respond with multiple locations from which the requester can choose. For successive requests for the same resource, the RNS server may respond with different sets of locations, selecting sets of locations in, for instance, a round robin fashion, in order to balance the network traffic to multiple locations. In one embodiment, the RNS server may select the locations to be returned in **230** based on the requester's network (IP) address, in order to provide the requester with addresses that are "proximal" in terms of network topology, and thus optimize network traffic.

← [Note the providing of addresses that are "proximal" in terms of network topology, in order to optimize

the network traffic. Logically, a node within a LAN is closest if it is located within a LAN in view of Internet, WAN and/or external network. In other words, the determination by the server that the first and second nodes are part of the same private network can be obtained by locating the closest and/or proximal node in terms of network topology].

In other words, the RNS server receives a search request for a resource from one of the peer, e.g. [0045], RNS server determines that the file is stored on one or more locations or peers by checking its own memory for resource records, e.g. [0046], and in an event of a positive determination, the RNS server responds with the status and set of locations where the resource is found to the requesting peer, e.g. [0047].

Moreover, Teodosiu, in one embodiment discloses that the **RNS server may select the locations to be returned based on the requester's IP address in order to provide the requester with addresses that <u>are "proximal" in terms of network topology</u>, and thus <u>optimize network traffic</u>. (Emphasis added).**

For example:

Consider the following figure with alterations and/or indications for analysis purposes.

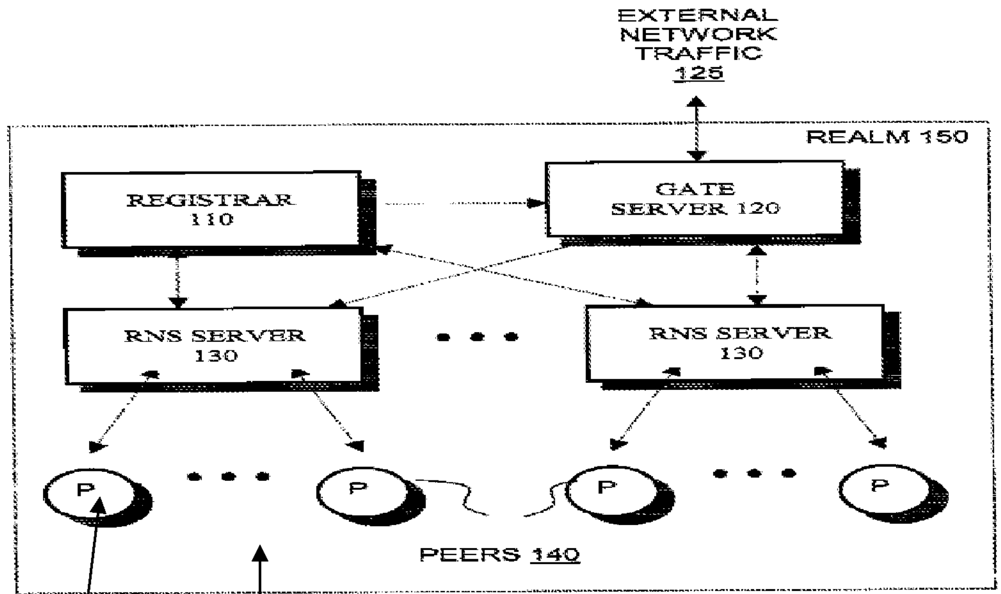

FIG. 1

Peer 1 Peer 2 Peer 3

In an event the real 150 is implemented over the LAN environment as set forth above, the peers 140 and/or peers 1-3 are said to be located within a LAN, i.e. same private network, and which are also part of peer to peer network.

In an event peer 1 initiates a search request for a resource that is located at peer 2 or 3 to RNS server, the RNS server will determine that the resource is located at one or more peers, for example, peer 2 and peer 3.

In one embodiment, e.g. [0047], when the RNS server utilizes the proximity criteria in <u>terms of network topology</u> to filter the locations and/or peers, the RNS server will respond to the search request for a resource with the locations that are closest to the requesting peer, i.e. closest in this case is the peer 2, in terms of network topology. Therefore, RNS server will respond to the requesting peer 1 with the locations of the peer 2, which are part of same private network.

However, Teodosiu does not literally disclose a process wherein RNS server determines that first node, i.e. requesting node, and a second node, i.e. node where resource can be found, are also part of same private network, such as local area network LAN.

Araujo

Araujo discloses a **process and/or a server that determines whether two nodes are part of the same private network,** i.e. whether the two nodes are part of the same LAN, e.g. fig. 5 item #511 and col. 7 L13-33, **as acknowledged by the appellant**, e.g. Brief, pg. 11, D. 1.

In other words, Araujo discloses a technique of determining by a server whether two nodes are included and/or part of the same LAN.

Modification

Teodosiu discloses peer to peer network comprising two or more peers, which are part of the peer to peer network and part of the private LAN, i.e. same private network.

Moreover, Teodosiu discloses sending the locations of the resource that are closest and/or proximal in terms of network topology to the requesting peer in order to optimize network traffic.

Araujo discloses determining whether two nodes in a network are part of the same LAN, i.e. same private network.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Teodosiu, more specifically, to modify RNS server to incorporate the process of determining whether the two peers are part of the same LAN.

See KSR International Co. v. Teleflex Inc., 550 U.S. ___,___, 82 USPQ2d 1385, 1395-97 (2007) identified a number of rationales to support a conclusion of obviousness which are consistent with the proper "functional approach" to the determination of obviousness as laid down in Graham. The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit, and **MPEP 2143. [** EXEMPLARY RATIONALES:

> Exemplary rationales that may support a conclusion of obviousness include:
> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable].

Hence, the combination of Teodosiu and Araujo explicitly discloses a server, e.g. RNS server, which would determine that the first peer and second peer, which in fact are part of the peer to peer network, are also part of the same LAN.

In the Brief, appellant submits that Araujo does not disclose that the devices in the same LAN are part of a peer to peer network, e.g. Brief, pg. 11.

In view of these arguments, it seems that the appellant is attempting to show nonobviousness by arguing and/or attacking references **individually because the appellant ignores** the fact that Teadosiu discloses the peer to peer network comprising peers located in the same LAN, i.e. devices in the same LAN are part of the peer to peer network.

As such, it should be noted that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., Inc., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)". **MPEP 2145 IV.**

(i) Particularly, the patent office has acknowledged that Teodosiu does not disclose that a server determines...Thus, the Patent office has implicitly acknowledged that Teodosiu does not disclose that a server determines that first and second nodes are part of the same private network, where the first and second nodes, which are part of the same private network, are also part of a peer-to-peer network (Brief, pg. 13).

In response to appellant's analysis, Examiner respectfully disagrees.

There is no indication whatsoever in any of the previous office actions that the patent office has implicitly, logically or explicitly acknowledged that Teodosiu does not disclose…" as asserted by the appellant in (i).

In the rejection, e.g. Final Action, pg. 7, Examiner clearly indicated that Teodosiu does not disclose **the process** of determining by a server that the first node and second nodes are part of the same private network.

This does not mean, whether interpreted implicitly, logically and/or explicitly, that "Teodosiu does not disclose that a server determines that first and second nodes are part of the same private network, where the first and second nodes, which are part of the same private network, are also part of a peer-to-peer network".

As set forth above, two nodes which are part of peer to peer network, can easily be part of same private network such as LAN, as acknowledged and/or admitted by the appellant in the background of rejection, which is reproduced above, as well as set forth in Teodosiu.

b. None of the references, either alone or in combination, disclose or suggest determining by a server that first and second nodes, which are part of a peer-to-peer network, are also part of a same private network…While Yau does disclose checking for source clients, which are behind the same firewall as a requesting client, neither of these clients are part of a peer to peer network (Brief, pg. 14 paragraph G. 1, pg. 15-17).

In response to argument [b], Examiner respectfully disagrees.

In light of the appellant's background of Invention section, first, it’s well know that peer to peer network have peers or users that are part of a private network, i.e. same private network. That is, two or more users from same LAN can participate in peer to peer network.

Secondly, Dutta, in a similar way as Teodosiu, also discloses implementing the peer to peer network over different types of networks including LAN, Internet, WAN, Intranet, etc., e.g. col. 3 L10-50 and fig. 4.

In other words, two or more peers within and/or part of a same LAN or intranet, i.e. same private network, are also part of the peer to peer network.

Yau et al.

Yau discloses:

[0018] It is an advantage of the invention to provide an improved system and method for distributing data to multiple nodes on a network efficiently by utilizing the network bandwidth of the recipient nodes. This approach reduces the bandwidth and system requirements of a centralized server or a distributed set of servers utilized by the data source. In addition to lowering costs associated with a centralized data source server, the invention can also reduce overall delivery time to recipients.

[0019] Another advantage of the invention is that it provides a method and system for the coordination of data transfers within a protected network, where the data source resides outside the protected network. This method allows computers networked behind a firewall server to receive data from external sources, such as computers connected to the Internet, without having to perform transfers through the firewall for each computer. Another benefit of this aspect of the invention is that data can be transferred at the usually higher local area network (LAN) rate of the protected network, rather than the external network rate.

In other words, Yau improves the network efficiency in distributing data to plurality of clients by enabling the requesting client to request the data from the client in the same private network, without having to perform transfers through distal and/or external computers.

In appellant's terms, Yau discloses a technique for optimizing private network file transfers comprising determining by the server whether the first, i.e. requesting client, and second client, client who has data, are located within the same private network which is protected by the firewall, as evidenced in the following figure, more specifically, in step 630.

600

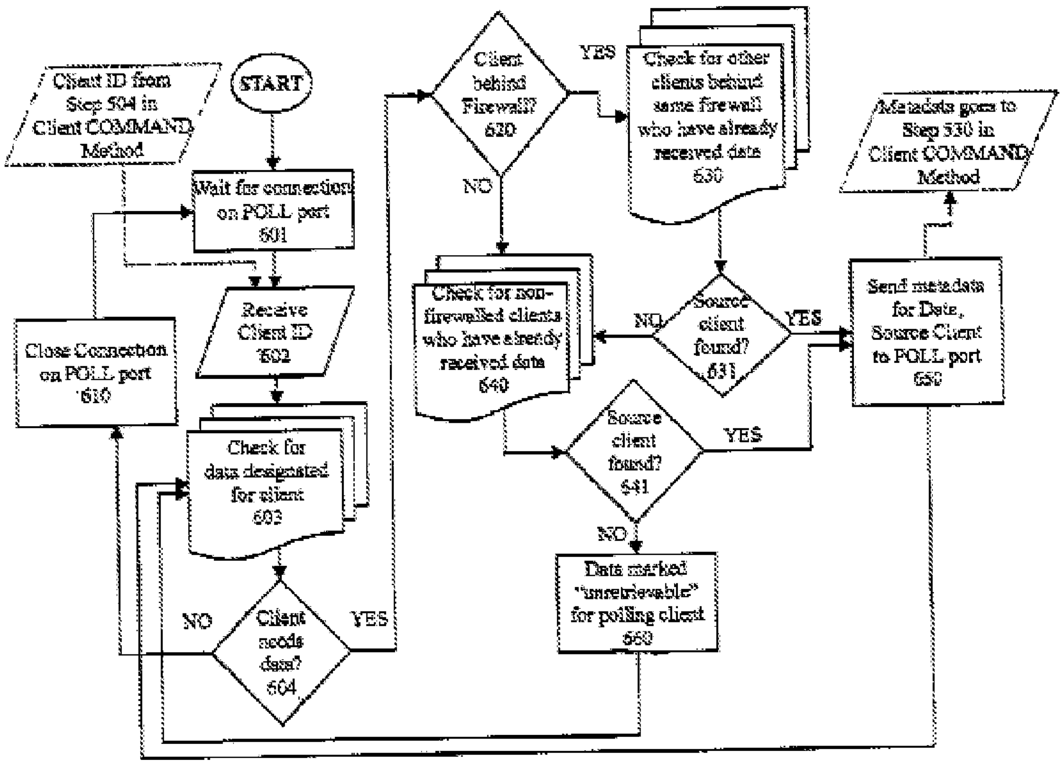

Figure 6

A firewall device is a well known device in the art used for securing the internal network such as LAN, intranet, etc., as evidenced in the following figure by item #82.

Generally, in the networking art, when the two devices are located within and/or connected to a same firewall, then the two devices are said to be located within a same private network.

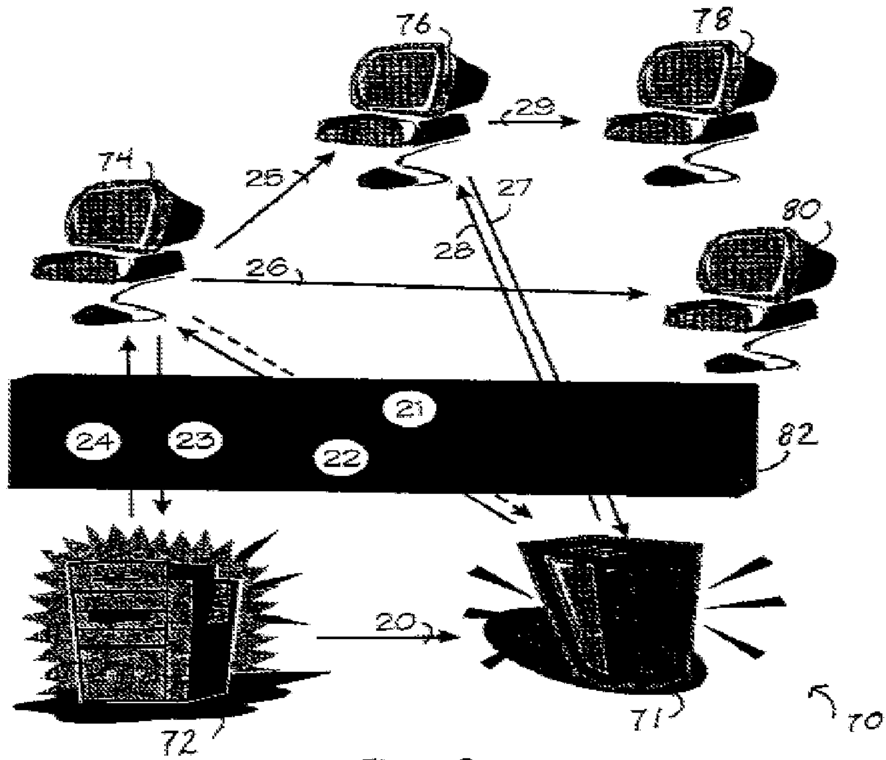

Figure 2

The network of devices such as device 74, 76, 78 and 80 is known as internal protected network and/or simply a private network, see also pg. 2 [0026].

[0026] **FIG. 2** shows a system **70** in accordance with another embodiment of the invention. The system **70** of **FIG. 2** is similar to the system **50** of **FIG. 1**. However, the system **70** of **FIG. 2** includes a firewall server **82**. In the system **70**, the clients **74-80** are connected to and communicate over a protected network behind the firewall **82**. The firewall **82** separates the network connecting the clients **74-80** from the network connecting the initial content-providing server **72** and the distribution-coordinating server **71**. Specifically, the firewall **82** can be configured to prohibit external connections to the clients **74-80**, and only allow connections from the clients **74-80** to nodes on the external network, where servers71-72 are located.

In other words, clients behind the firewall are located within an internal and/or private network, whereas, servers 72-71 are located on the external network and/or non-private network.

The invention of Yau, in part, works as follows:

[0066] **FIGS. 6 and 7** describe the functionality of the distribution-coordinating servers **51, 71** shown in FIGS. **1-2**. The role of the servers **51,71** is to coordinate transactions between clients to ensure that clients on a distribution list receive data intended for them. The servers **51, 71**, which can be implemented using one or more computers, keep track of nodes that have data, and facilitate the transmission of that data to those nodes that request the data but do not yet have it. Distribution lists and records of clients requesting data and those clients storing data can be stored in databases accessible to the servers **51, 71**.

[0067] The distribution-coordinating servers **51,71** can be configured to determine optimal data flow across the network. Optimal data distribution rates can be determined based on a number of useful heuristics, such as network topology, relative bandwidths between nodes, and physical locations of nodes.

[0068] **FIG. 6** is a flowchart **600** illustrating a polling operation of a distribution-coordinating server includable in the networks of FIGS. **1-2**. The method, referred to herein as the Server POLL method, describes how the distribution-coordinating server can instruct a client to retrieve, i.e., pull, data from another source (usually another client). Since data is usually pushed to clients by default rather than having clients pull the data themselves, a client would only need to invoke this server-side method in circumstances in which other clients are unable to push data to it. Such circumstances arise when a client is behind a firewall, or when it first subscribes to a service and needs to be added to a distribution list.

[0069] In step **601**, the distribution-coordinating server waits for clients to invoke its Server POLL method by requesting a connection on the server's POLL port. When a client requests a connection, the server identifies the client by receiving its metadata (step **602**).

[0070] The server then checks whether the client is on a distribution list for a particular piece of data but has not yet received that data (steps **603-604**). If the server's records show no data destined for the client, the server closes the connection with the client (step **610**) and returns to waiting for new connections (step **601**).

[0071] If the client needs data, however, the server then looks for a node from which the client can retrieve this data, referred to in the flowchart as the source client. A check is made to determine whether the client is behind a firewall (step **620**). The coordinating server can compare the IP address of the client to determine whether the client resides behind a firewall. Specifically, the server can store a list of IP addresses for firewall servers. If the IP address of the client corresponds to one of the firewalls in the list, then the coordinating server can treat the client as a firewalled client.

[0072] If the client is a firewalled client, the coordinating server first checks for source clients behind the same firewall that already have the data (step **630**), and uses such a client if it exists (step **631**). A source client behind the same firewall allows the system to take advantage of the higher speeds usually achieved by subnets and to aid in the ability to propagate data throughout subnets protected by firewalls.

[0073] If the client is not firewalled, or if no other clients behind the firewall have the desired data, the server searches its records for a non-firewalled client that has the data (step **640**).

[0074] If a source client is successfully found, the server refers the client to the source client by sending it metadata to identify the data and the location of the source client from which it should retrieve the data (step **650**). On the other hand, if a suitable source client is still not found, the server can mark the data as temporarily irretrievable by the polling client (step **660**), or permanently irretrievable if a suitable source client is not found after repeated attempts.

In other words, **the distribution-coordinating servers** determines the optimal data flow across the network, e.g. [0067], through checking for the node within the same private network

from which the client can retrieve data, by determining whether the client and the node is behind the same firewall, i.e. determines whether the client, i.e. first node and the source node, i.e. second node, are part and/or are located within the same internal or private network protected by the firewall, e.g. [0071-0072], and instructs the client to retrieve the data from the source node by sending the metadata and the location of the source client, e.g. [0074].

Clearly, Yau discloses the server and the process of determining whether the two nodes are located within and/or are part of the same private network such as an internal network **in order to optimize the data distribution and/or transfers.**

In fact, Yau discloses the same technique for achieving the optimal file transfer and/or data flow as disclosed in the present application with respect to peer to peer networks.

As such, the combination of Dutta and Yau, wherein Dutta discloses a peer to peer network comprising two or more devices located within the same LAN or private intranet and Yau discloses a server that determines whether the two nodes are part of the same internal network, does teach and disclose determining, by a server that first and second nodes are part of a same private network, where the first and second nodes are part of a peer to peer network.

Furthermore, the rational for the combination can be found in the following:

> **KSR International Co. v. Teleflex Inc.**, 550 U.S. ___,___, 82 USPQ2d 1385, 1395-97 (2007) identified a number of rationales to support a conclusion of obviousness which are consistent with the proper "functional approach" to the determination of obviousness as laid down in Graham. The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit, and **MPEP 2143. [** EXEMPLARY RATIONALES:

Exemplary rationales that may support a conclusion of obviousness include:
(A) Combining prior art elements according to known methods to yield predictable results;
(B) Simple substitution of one known element for another to obtain predictable results;
(C) Use of known technique to improve similar devices (methods, or products) in the same way;
(D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
(E) "Obvious to try" – choosing from a finite number of identified, predictable].

For example: In the present prima facie case of obviousness and/or combination, rationale (A) and (C) applies.

In the Brief, appellant alleges that "while Yau disclose checking for source clients, which are behind the same firewall as a requesting client, neither of these clients are part of peer to peer network".

In view of this argument, it seems that appellant is attempting to show nonobviousness by arguing and/or attacking references individually because appellant ignores the fact that Dutta discloses the peer to peer network comprising peers located in the same LAN, i.e. devices in the same LAN are part of the peer to peer network.

MPEP 2145 IV clearly discloses that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., Inc., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)". **MPEP 2145 IV.**

In summary, the combination of Teodosiu and Araujo, and/or the combination of Dutta and Yau teaches achieving optimization of data transfer in peer to peer networks by realizing that the requesting node and responding node, i.e. node having the requested file, are located within the same private network and enabling the requesting node to retrieve the file from the closest node and/or node located within the same private network such as LAN.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Kamal Divecha
Art Unit 2151
/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151

Conferees:

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2146